

SEALED

UNITED STATES DISTRICT COURT

CLERK'S OFFICE U.S. DIST. COURT
AT CHARLOTTESVILLE, VA
FILED

for the

Western District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Various electronic devices seized from 2423 South
Holland Sylvania Road, Apt. 219, Maumee, Ohio on
August 13, 2017

Case No.

3:17mj00041

AUG 16 2017

JULIA C. DUDLEY CLERK

BY:

DEPUTY CLERK

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Various electronic devices seized from 2423 South Holland Sylvania Road, Apt. 219, Maumee, Ohio on August 13, 2017 currently located in evidence storage of the Charlottesville FBI office (See Attachment A)

located in the Western District of Virginia, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. 249

Offense Description

Willfully cause bodily injury to any person, or through the use of a dangerous weapon attempts to cause bodily injury to any person, because of the actual or perceived race, color, religion, or national origin of any person

The application is based on these facts:
See attached affidavit of Special Agent Johnny Mac Lavender II with the Federal Bureau of Investigation

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

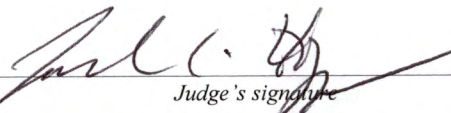
Special Agent Johnny Mac Lavender II, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/16/2017

City and state: Charlottesville, Virginia



Judge's signature

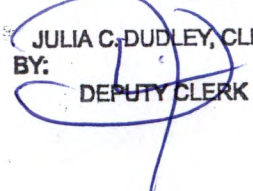
Honorable Joel Hoppe, United States Magistrate Judge

Printed name and title

SEALED

CLERK'S OFFICE U.S. DIST. COURT
AT CHARLOTTESVILLE, VA
FILED

AUG 16 2017

JULIA C. DUDLEY, CLERK
BY:  DEPUTY CLERK

IN THE
UNITED STATES DISTRICT COURT
FOR THE
WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE VIRGINIA

IN THE MATTER OF THE SEARCH OF
VARIOUS ELECTRONIC DEVICES
SEIZED FROM 2423 SOUTH HOLLAND
SYLVANIA ROAD, APT. 219, MAUMEE,
OHIO ON AUGUST 13, 2017

Case No.

3:17mj00041

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Johnny Mac Lavender II, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of various electronic devices, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (hereinafter the "FBI"), and have been since July 2002. I have participated in and have experience in the investigation of various federal criminal violations, to include domestic terrorism, white-collar crimes, and civil rights violations. I have also participated in searches, authorized by consent or by search warrant, of residences, commercial premises, vehicles, cell phones, and other locations for documentary evidence. Through training and experience, your affiant has knowledge that

Reviewed by Asa Rnaly M. Heber, 8-16-2017

persons affiliated with white supremacists groups and/or conspirators will utilize computers and other electronic devices to conduct their illegal activity and maintain contact with other confederates, conspirators and criminal associates involved with the planning, targeting and execution of their political or social goals, to include – but not limited to – espousing, inciting, encouraging, inducing, or engaging in acts of violence.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is:

- **ALIENWARE CPU S/N 8443979210;**
- **WD Blue External Hard Drive S/N WCC6Y2HNU8T4;**
- **ALIENWARE LAPTOP S/N 2VMDK32;**
- **PNY ATTACHE FLASH DRIVE 1G – PURPLE IN COLOR**
- **PNY FLASH DRIVE 4GB – RED IN COLOR**
- **NETGEAR ROUTER 4841515303D34;**
- **CPU BLACK #053316469707;**
- **SEAGATE EXTERNAL HARD DRIVE S/N NA7PRCKP;**
- **PLAYSTATION 3 S/N CK025451603;**
- **X-BOX S/N 038323253308;**

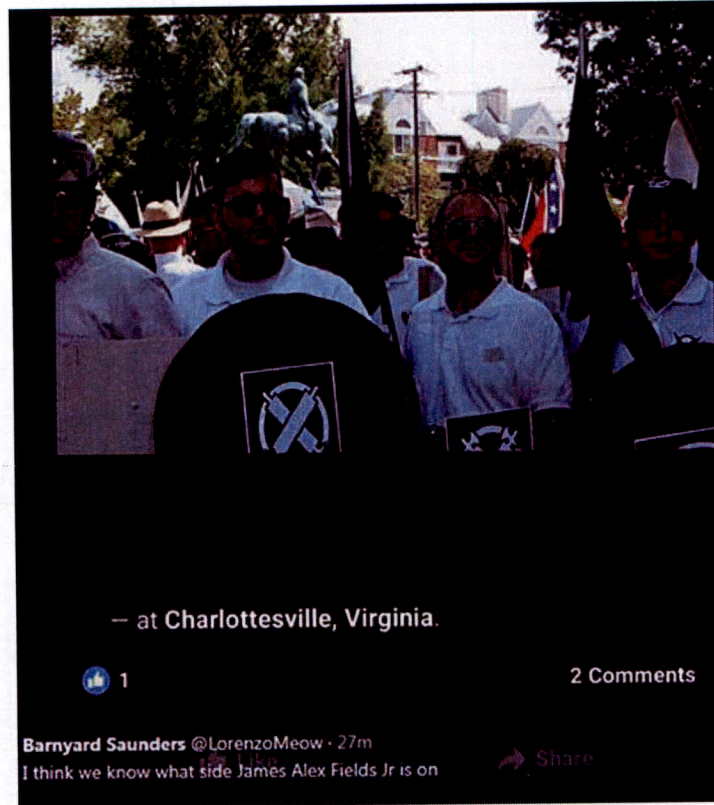
hereinafter the “**Devices.**” The **Devices** are currently located in evidence storage at the FBI Charlottesville Resident Agency located at 2211 Hydraulic Road, Suite 201, Charlottesville, Virginia, within the Western District of Virginia.

5. The applied-for warrant would authorize the forensic examination of the **Devices** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. JAMES ALEX FIELDS has been identified as the operator of a grey Dodge Charger, bearing Ohio license plate GVF1111, who on August 12, 2017 drove his vehicle into a crowd of African Americans, Black Lives Matter (“BLM”) supporters, and other like-minded protestors, killing one Caucasian female and injuring approximately twenty other individuals of African-American and Caucasian descent. Based on your affiant’s review of the video footage of the incident, your affiant believes that the vehicle was traveling at a high rate of speed intending to strike protestors, including African Americans and BLM supporters. After striking multiple victims with his vehicle, FIELDS then began to drive his vehicle backwards, in reverse, at a high-rate of speed to flee the scene.

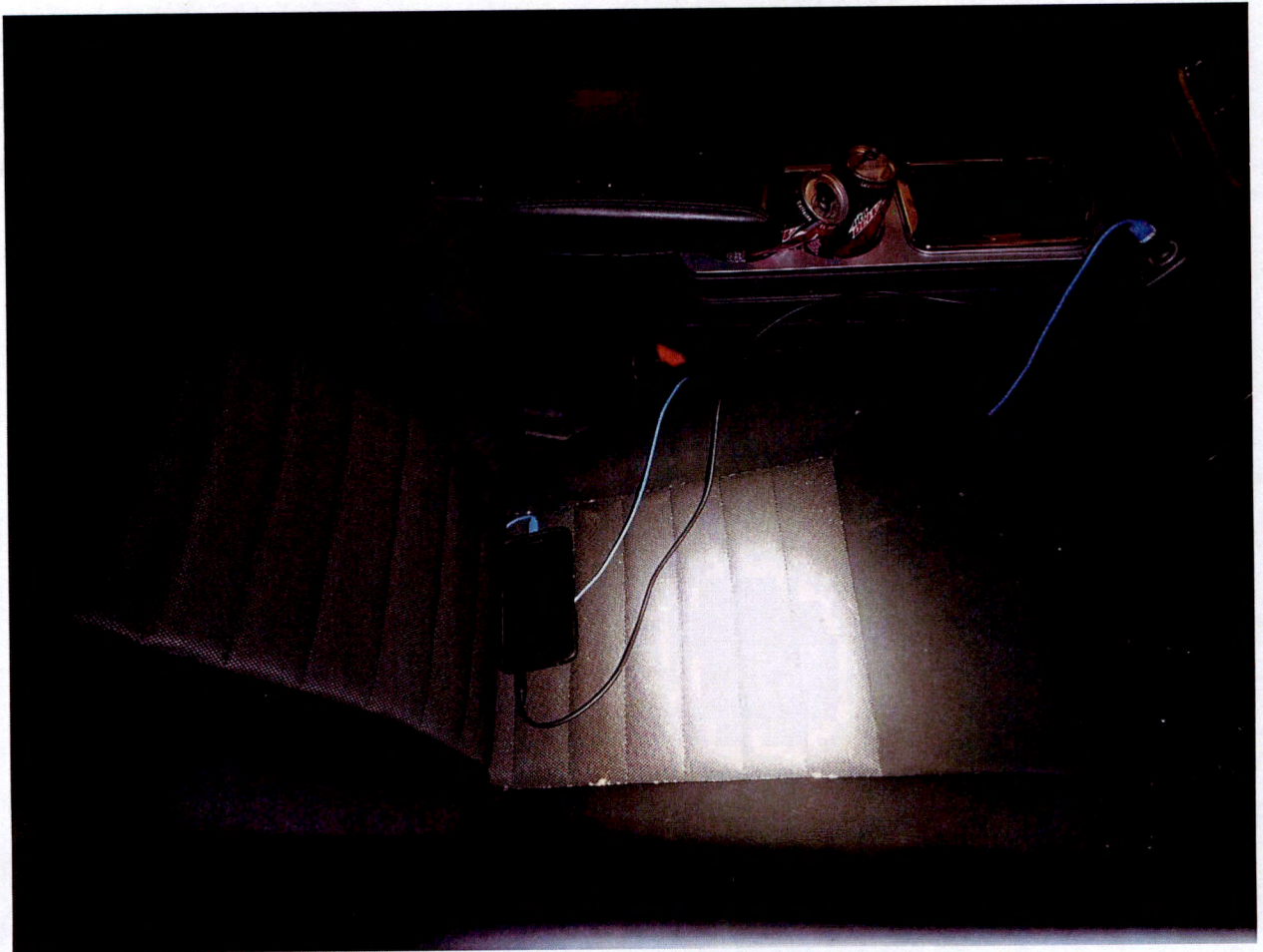
7. Your affiant knows from other law enforcement officers that FIELDS was dressed in a white polo shirt, khaki pants, and black shoes after his arrest at the Charlottesville Police Department. FIELDS’ hair was trimmed with a “high and tight” or “side-fade” style consistent with the hairstyle of other individuals associated with the white supremacist group Vanguard America at the rally. Below is a picture of FIELDS law enforcement obtained from social media at the Charlottesville “Unite the Right” rally. FIELDS is second person from the left with the large black shield in front of him.



8. Your Affiant knows from other law enforcement that FIELDS was the only person in the vehicle at the time of this incident. After the Charlottesville Police Officers arrested FIELDS, the vehicle was towed and stored in a secured law enforcement facility. Your affiant has observed a copy of the Ohio Motor Vehicle Registration that identifies FIELDS as the registrant and provides the address: 6853 Deer Ridge Road, Apartment 16, Maumee, Ohio, Lucas County. Your affiant knows from other law enforcement officers that FIELDS' mother SAMANTHA BLOOM is the current resident at the Deer Ridge Road address. During an interview on August 12, 2017, BLOOM stated that FIELDS currently lives alone at the address 2423 Holland Sylvania Road S. Apt 219, Maumee, Ohio.

9. The Charlottesville Police Department obtained a Virginia State search warrant for this vehicle and collected one Samsung cellular phone lying on the front passenger seat. The

cellular phone was plugged in to the outlet and would be accessible to the driver of the vehicle as seen below.



10. Your Affiant knows from training and experience that individuals use cellular phones to communicate with friends, family, and acquaintances. Today's cellular phones can communicate a number of ways to include text messages, incoming and outgoing calls, through social media, text applications and routinely use their phone as a camera and video camera.

11. On or about August 13, 2017 a federal search warrant was executed by special agents of the Federal Bureau of Investigation in the Northern District of Ohio on FIELDS' residence located at 2423 South Holland Sylvania Road, Apartment 219, Maumee, Ohio 43537. The residence was a one-bedroom apartment, and there was no indication that any other

individuals resided at the location. Located in the apartment was a large framed picture of Adolph Hitler, a copy of *Mein Kampf*, and other items associated with the Nazi movement. The **Devices** were all located within these premises, and were seized pursuant to the execution of the search warrant. Therefore, even though the FBI might already have all necessary authority to examine the **Devices**, I seek this additional warrant out of an abundance of caution to be certain that an examination of the **Devices** will comply with all relevant and applicable laws.

12. The **Devices** are currently in evidence storage at the FBI Charlottesville Resident Agency, located at 2211 Hydraulic Road, Suite 201, Charlottesville, Virginia, within the Western District of Virginia. In my training and experience, I know that the **Devices** have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **Devices** first came into the possession of the FBI.

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- b. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- c. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- d. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, I know that all of the Devices listed above have capabilities that allow it to store content and identifying information that would serve as relevant evidence into this investigation. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used a particular device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. There is probable cause to believe that things that were once stored on the **Devices** may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Devices** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

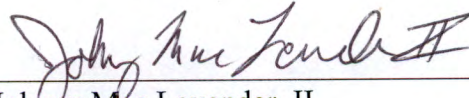
18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

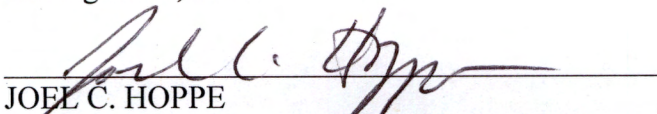
20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Johnny Mac Lavender, II
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on August 16, 2017:


JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE